Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

17 October 2017

PIN Number

171017-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@ic.fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This PIN has been released TLP: GREEN: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Medical Device Vulnerabilities Pose Growing Risk to US Healthcare Services and Patient Care

Summary

This year's WannaCry (WCry), aka WanaCrypt 2.0 ransomware attack marked the first FBI observed cyber attack that affected medical device operability in the United States. Medical devices were especially vulnerable to the WCry attack due to their reliance on outdated, unsupported software. Medical devices almost certainly will remain vulnerable to cyber attacks exploiting such software.

Threat

The increased connectivity of medical devices and healthcare networks invariably increases cyber intrusion risks from a variety of vectors. Cyber attacks targeting software vulnerabilities could cause widespread disruptions to US healthcare operations, especially because of the interconnectivity of devices throughout healthcare networks. In May 2017, WCry infected at least 200,000 systems in more than 150 countries worldwide by exploiting a known vulnerability in the Windows operating system (OS) and self-propagating to other vulnerable systems on host networks. By the end of the month, the Healthcare and Public Health Sector represented half of the identified US WCry victim organizations. According to FBI reporting and threat response activities, multiple US organizations suffered operational disruption to medical devices which impacted healthcare services - including computed tomography (CT) scanners and injection systems and radiology scan viewing workstations. In some instances, devices had to be removed from the network for remediation while other cases required the transfer of patients to other facilities for continued services, resulting in a delay of care.

The ransomware attack highlighted the industry's challenges to provide timely patching and remediation for medical devices software. For example, in the case of WCry, Microsoft released a Windows 7 security patch several months earlier to protect against such an attack, but healthcare providers were victimized because some medical devices operated on other unsupported Windows versions. Based on FBI assessments from the WCry attack, contributing factors to medical device vulnerabilities include (but are not limited to) the following:

- Many devices rely on commercial off-the-shelf software and do not receive routine, if any, security testing or updates.
- If not clearly defined in vendor agreements, responsibility for post-market device cybersecurity is often unclear between manufacturers, vendors, and healthcare providers.
- Manufacturers, vendors, and providers may not have a full or accurate understanding of the requirements for deploying cyber security updates and the potential impact (if any) updates could have on devices' US Food and Drug Administration (FDA) clearance or approval.
- Providers depend heavily on compensating control measures, such as increased network defense tactics and use of virtual local area networks, to provide security for devices on their networks. However, secure device implementation can be difficult given the complexity of device systems and provider network environments, especially without effective change management policies.
- It is challenging for manufacturers to change a device's technology base (e.g., operating system) or even anticipate when the current base will become obsolete, given the long development process and service lifetime of many devices.
- Market demand for security devices is lacking, as manufacturers generally have not advertised the benefits of device cybersecurity and few providers have taken a stance against purchasing unsecure devices.

Recommendations:

Healthcare providers, medical device manufacturers, and device vendors who (a) clearly define cybersecurity responsibilities through provider/vendor agreements, (b) implement changes necessary to develop, enforce, and maintain device security, and (c) proactively communicate cybersecurity challenges between one another, are more likely to avoid falling victim to cyber attacks against medical devices and healthcare networks. The FBI leads and encourages participation in the Cyber Health Working Group through the InfraGard Program, which encourages IT professionals in the healthcare industry to share real-time tactical information about threats, trends, and best practices.[a]

The FDA provides pre[b] and post[c] -market guidance for the management of cybersecurity in medical devices. An “FDA Fact Sheet” is available online detailing the FDA’s role and addressing many of the misconceptions surrounding medical device cybersecurity issues.[d] In addition, medical device stakeholders are encouraged to reference the recently published UL 2900-1, Standard for Software Cybersecurity Network-Connectable Products, Part I: General Requirements (effective 21 August 2017).

The Department of Homeland Security (DHS), US-CERT, and the Department of Health and Human Services provide additional resources for government and industry cybersecurity support. Information is available on their respective Web sites.

Healthcare organizations should consider general cyber best practices to evaluate their network security and protect their systems. The following list includes self-protection strategies which could help reduce unauthorized network access:

- Scrutinize links contained in e-mails, and do not open attachments included in unsolicited e-mails.
- Disable macros. Be careful of pop-ups from attachments that require users to enable them.

[a] For more information, visit www.intelligence.healthcare/

[b] Content of Premarket Submissions for Management of Cybersecurity in Medical Devices https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

[c] https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

[d] For more information, visit https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM544684.pdf

- Only download software–especially free software–from known and trusted sites.
- Create a centralized e-mail account for employees to report suspicious e-mails.
- Change network default passwords, configurations, and encryption keys. Use strong, complex passwords or passphrases.
- Do not use the same login and password for multiple platforms, servers, or networks.
- Recommend your organization's IT professional(s) review, test, and certify the need/compatibility of a patch or update prior to installing it onto the operating system or software.
- Implement two-factor authentication for access to sensitive systems.
- Restrict access to the Internet on systems handling sensitive information or operations. If possible, isolate sensitive systems only within the network.
- Only allow required processes to run on systems handling sensitive information and operations.
- Install and regularly update anti-malware solutions, software, operating systems, remote management applications, and hardware.
- Monitor unusual traffic, especially over non-standard ports.
- Ensure remote desktop protocol configurations are changed from their default settings.
- Monitor outgoing data, and be willing to block unknown IP addresses.
- Ensure proper firewall rules are in place.
- Be aware of the organization's footprint and persona facing the Internet. Conduct searches using multiple search engines on multiple Internet domains of the organization's names, Web addresses, and key personnel to determine if there is an unidentified weak point in the network security. Conduct infrastructure look-ups in the public domains to ensure additional information is not inadvertently advertised.

Reporting Notice:

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field Office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or by e-mail at cywatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Suspected device-associated deaths, serious injuries, and malfunctions should be reported to the FDA via the Medical Device Reporting (MDR) Web page. A variety of mandatory medical device reporting requirements exist for manufacturers, importers, and device user facilities.

Healthcare professionals, patients, caregivers, and consumers may voluntarily report significant adverse events or product problems with medical products via MedWatch, the FDA's Safety Information and Adverse Event Reporting Program, or through the MedWatcher mobile app. For MDR guidance, including interpretation of MDR policy, contact the FDA by phone at 301-796-6670 or e-mail at MDRPolicy@fda.hhs.gov.

Administrative Note

This product is marked TLP:GREEN. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released outside of the community.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey